	• • • • • • • • • • • • • • • • • • • •		• • • • • • • • • • • • • • • • • • • •		• • •
	(Origin	al Signat	ure of Me	ember)	

107TH CONGRESS 2D SESSION

H.R.

To protect and enhance consumer privacy, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. Stearns (for himself, Mr. Boucher, Mr. Tauzin, Mr. Towns, Mr. Bass, Mr. Bilirakis, Mrs. Bono, Mr. Deal of Georgia, Ms. Eshoo, Mr. Gillmor, Mr. Gordon, Mr. Greenwood, Mr. Kingston, Mr. Moran of Virginia, Mr. Sawyer, Mr. Terry, Mr. Upton, Mr. Walden, Mr. Weldon of Florida, and Mr. Weller) introduced the following bill; which was referred to the Committee on

A BILL

To protect and enhance consumer privacy, and for other purposes.

- 1 Be it enacted by the Senate and House of Representa-
- 2 tives of the United States of America in Congress assembled,
- 3 SECTION 1. SHORT TITLE.
- 4 This Act may be cited as the "Consumer Privacy Pro-
- 5 tection Act of 2002".



1 SEC. 2. TABLE OF CONTENTS.

2 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.

TITLE I—PROTECTION OF INDIVIDUAL PRIVACY IN INTERSTATE COMMERCE

- Sec. 101. Privacy notices to consumers.
- Sec. 102. Privacy policy statements.
- Sec. 103. Consumer opportunity to limit sale or disclosure of information.
- Sec. 104. Consumer opportunity to limit other information practices.
- Sec. 105. Information security obligations.
- Sec. 106. Self-regulatory programs.
- Sec. 107. Enforcement.
- Sec. 108. No private right of action.
- Sec. 109. Effect on other laws.
- Sec. 110. Effective date.

TITLE II—IDENTITY THEFT PREVENTION AND REMEDIES

- Sec. 201. Facilitating electronic identity theft affidavits.
- Sec. 202. Promoting use of common identity theft affidavit.
- Sec. 203. Timely resolution of identity theft disputes.
- Sec. 204. Improvements to consumer clearinghouse.
- Sec. 205. Improved identity theft data.
- Sec. 206. Change of address protections.
- Sec. 207. Effective date.

TITLE III—INTERNATIONAL PROVISIONS

- Sec. 301. Study by Comptroller General.
- Sec. 302. Remediation of discriminatory impact by Secretary of Commerce.
- Sec. 303. Effect of nonremediation.
- Sec. 304. Harmonization of international privacy laws, regulations, and agreements.

TITLE IV—GENERAL PROVISIONS

Sec. 401. Definitions.



1 TITLE I—PROTECTION OF INDI-

2 VIDUAL PRIVACY IN INTER-

3 **STATE COMMERCE**

- 4 SEC. 101. PRIVACY NOTICES TO CONSUMERS.
- 5 (a) Notice Required.—A data collection organiza-
- 6 tion shall provide to a consumer a notice containing the
- 7 information required under subsection (b) as follows:
- 8 (1) Upon the first instance of collection from
- 9 the consumer of personally identifiable information,
- that may be used for a purpose unrelated to the
- transaction, by a data collection organization, the or-
- ganization shall provide the notice at the time per-
- sonally identifiable information is collected.
- 14 (2) Upon a material change in the organiza-
- tion's privacy policy statement under section 102(5),
- the organization shall provide the notice, not later
- than the first time after such change in policy that
- the organization seeks to collect, sell, disclose for
- 19 consideration, or use personally identifiable informa-
- 20 tion to the extent practicable, to each consumer from
- whom the organization has collected such informa-
- tion.
- 23 (b) FORM AND CONTENTS OF NOTICE.—A notice re-
- 24 guired under subsection (a) shall be provided in a clear
- 25 and concise manner, be prominently displayed or explicitly

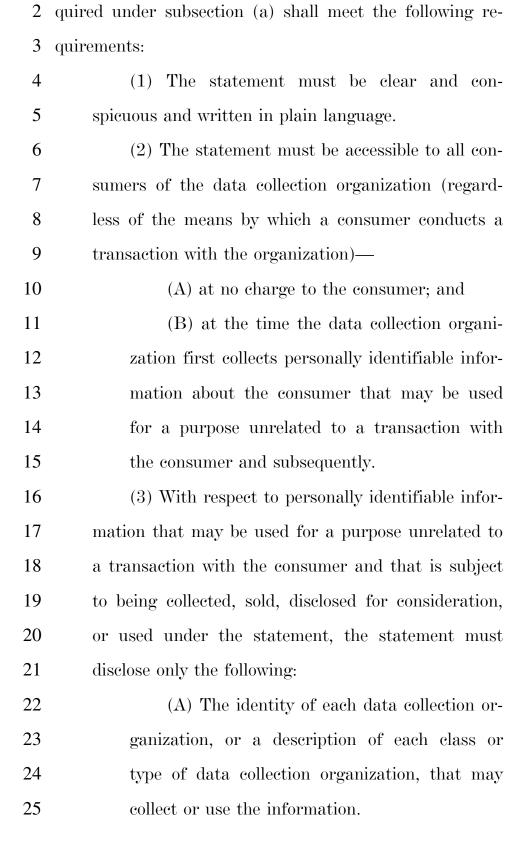


1	stated to the consumer, and contain the following informa-
2	tion:
3	(1) A statement that the information privacy
4	practices of the data collection organization raise an
5	issue of privacy for the consumer that may provide
6	the consumer with rights under law.
7	(2) A description of the manner in which the
8	consumer may obtain a privacy policy statement that
9	meets the requirements of section 102, which may
10	include providing the consumer with an Internet
11	website, a hyperlink to such a website, or a toll-free
12	telephone number from which such a statement may
13	be obtained.
14	(3) If the notice is required under subsection
15	(a)(2), a statement that there has been a material
16	change in the organization's privacy policy.
17	SEC. 102. PRIVACY POLICY STATEMENTS.
18	(a) Privacy Policy.—A data collection organization
19	shall establish a privacy policy with respect to the collec-
20	tion, sale, disclosure for consideration, or use of the per-
21	sonally identifiable information of consumers, the prin-
22	cipal elements of which shall be embodied in a privacy pol-
23	icy statement (or statements) that meets the requirements
24	of subsection (b).



1

(b) Statement.—The statement (or statements) re-





	Ÿ
1	(B) The types of information that may be
2	collected, sold, disclosed for consideration, or
3	used.
4	(C) How the information may be used.
5	(D) Whether the consumer is required to
6	provide the information in order to do business
7	with the data collection organization.
8	(E) The extent to which the information is
9	subject to sale or disclosure for consideration to
10	a data collection organization that is not an in-
11	formation-sharing affiliate of the data collection
12	organization providing the statement, including
13	the following:
14	(i) A clear and prominent statement
15	of the fact that the information is subject
16	to such sale or disclosure for consideration.
17	(ii) A description of each class or type
18	of data collection organization to which the
19	information may be sold or disclosed for
20	consideration.
21	(iii) The purpose for which the infor-
22	mation may be used.
23	(F) Whether the information security prac-
24	tices of the data collection organization meet

the security requirements of section 105 in



	·
1	order to prevent unauthorized disclosure or re-
2	lease of personally identifiable information.
3	(c) Commission Facilitation.—The Commission
4	shall take actions (including conducting industry-wide
5	workshops) to facilitate the development of harmonized,
6	universal wording or logo-based graphics in order to con-
7	vey the contents of privacy policy statements required
8	under this section.
9	SEC. 103. CONSUMER OPPORTUNITY TO LIMIT SALE OR DIS-
10	CLOSURE OF INFORMATION.
11	(a) Preclusion of Sale or Disclosure.—
12	(1) Requirement.—A data collection organi-
13	zation shall provide to the consumer, without charge,
14	the opportunity to preclude any sale or disclosure for
15	consideration of the consumer's personally identifi-
16	able information, that may be used for a purpose
17	unrelated to a transaction with the consumer, to any
18	data collection organization that is not an informa-
19	tion-sharing partner of the data collection organiza-
20	tion providing such opportunity.
21	(2) Duration.—A preclusion on sale or disclo-
22	sure for consideration of information established by
23	a consumer under this subsection shall remain in ef-
24	fect for 5 years or until the consumer indicates oth-

erwise, whichever occurs sooner. A data collection



1	organization may not seek reconsideration of a con-
2	sumer's preclusion of such sale or disclosure until at
3	least 1 year after such preclusion has been imposed
4	by the consumer.
5	(b) Permission for Sale or Disclosure.—A data
6	collection organization may provide the consumer an op-
7	portunity to permit the sale or disclosure described in sub-
8	section $(a)(1)$ in exchange for a benefit to the consumer.
9	(c) Accessibility.—The opportunity to preclude (or
10	if offered, to permit) the sale or disclosure for consider-
11	ation of information under this section must be both easy
12	to access and use.
13	SEC. 104. CONSUMER OPPORTUNITY TO LIMIT OTHER IN-
13 14	SEC. 104. CONSUMER OPPORTUNITY TO LIMIT OTHER INFORMATION PRACTICES.
14	FORMATION PRACTICES.
14 15	FORMATION PRACTICES. If a data collection organization provides to a con-
14151617	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data
14151617	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to collection or use of
14 15 16 17 18	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to collection or use of personally identifiable information regarding the con-
141516171819	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to collection or use of personally identifiable information regarding the consumer, other than that required by section 103—
14 15 16 17 18 19 20	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to collection or use of personally identifiable information regarding the consumer, other than that required by section 103— (1) that opportunity must be easy to access and
14 15 16 17 18 19 20 21	FORMATION PRACTICES. If a data collection organization provides to a consumer the opportunity to limit other practices of the data collection organization with respect to collection or use of personally identifiable information regarding the consumer, other than that required by section 103— (1) that opportunity must be easy to access and to use; and



1	(A) the limitation is withdrawn by the con-
2	sumer; or
3	(B) the data collection organization pro-
4	vides the consumer at least 30 days notice be-
5	fore terminating its compliance with the limita-
6	tion.
7	SEC. 105. INFORMATION SECURITY OBLIGATIONS.
8	(a) Information Security Policy.—
9	(1) Implementation.—A data collection orga-
10	nization shall prepare, revise as necessary, and im-
11	plement an information security policy that is appli-
12	cable to the information security practices and treat-
13	ment of personally identifiable information main-
14	tained by the data collection organization, in order
15	to prevent the unauthorized disclosure or release of
16	such information.
17	(2) Management approval.—An information
18	security policy created pursuant to paragraph (1)
19	shall be considered and approved by the senior man-
20	agement officials of the data collection organization
21	(3) Contents.—An information security policy
22	required under paragraph (1) shall include—
23	(A) a process for taking corrective action
24	pursuant to subsection (b); and



	10
1	(B) identifying an officer of the data col-
2	lection organization as the point of contact with
3	responsibility for information security issues for
4	the organization.
5	(b) Corrective Actions.—
6	(1) Notification and action.—Except as
7	provided in paragraph (2), upon the joint issuance
8	of an information security notification by a Federal
9	Government agency and the CERT Coordination
10	Center, a data collection organization shall take ap-
11	propriate action, within a reasonable period of time
12	after being informed and pursuant to its information
13	security policy, to implement any necessary changes
14	to its security practices and the architecture, instal-
15	lation, or implementation of its network or operating
16	software (including corrective patches) in response
17	to such a notification.
18	(2) Exceptions.—A data collection organiza-
19	tion shall not be required to take the action specified
20	in a notification under paragraph (1) if—
21	(A) the corrective action required would
22	cause harm to, or weaken, the organization's
23	existing information security for personally
24	identifiable information or the procedures or

systems of the organization;



1	(B) the organization takes, or has taken,
2	other appropriate steps or corrective action to
3	mitigate the vulnerabilities and exposure risks
4	identified in the notification; or
5	(C) the specified corrective action is not
6	necessary.
7	(3) CERT COORDINATION CENTER DE-
8	SCRIBED.—For purposes of this section, the CERT
9	Coordination Center is the Computer Emergency
10	Response Team Coordination Center of the Software
11	Engineering Institute operated by Carnegie Mellon
12	University in Pittsburgh, Pennsylvania, or if such
13	center is unavailable, an equivalent center des-
14	ignated by the Commission.
15	(c) Effect of Release of Personally Identifi-
16	ABLE INFORMATION.—If the security of a data collection
17	organization has been compromised, resulting in the unau-
18	thorized release of a consumer's personally identifiable in-
19	formation, the Commission shall treat the failure of the
20	data collection organization to comply with its own secu-
21	rity policy or respond to a Federal agency information se-
22	curity notification in accordance with subsection (b)(1) as
23	one factor in determining whether that data collection or-
24	canization has violated this section



SEC. 106. SELF-REGULATORY PROGRAMS.

1	SEC. 100. SELF-REGULATORT I ROGRAMS.
2	(a) Self-Regulatory Program.—
3	(1) Presumption of compliance.—The Com-
4	mission shall presume that a data collection organi-
5	zation is in compliance with the provisions of sec-
6	tions 101 through 105 if that organization—
7	(A) participates in a self-regulatory pro-
8	gram approved under subsection (b); and
9	(B) complies with the guidelines, proce-
10	dures, requirements, and restrictions of the pro-
11	gram (including a remedial process under sub-
12	section $(e)(7)$.
13	(2) Effect of Willful Noncompliance.—A
14	data collection organization that participates in a
15	self-regulatory program under this section shall not
16	be liable for a civil penalty arising out of a violation
17	of any provision of sections 101 through 105 unless
18	such violation results from willful noncompliance
19	with the guidelines, procedures, requirements, or re-
20	strictions of the program.
21	(b) Approval by Commission.—
22	(1) Approval.—The Commission shall, within
23	90 days after submission of an application for ap-

proval of a self-regulatory program under this sec-

tion (or of a material change in a program pre-

viously approved by the Commission), approve such



24

25

25

101 through 105.

	13
1	program (or change) if the Commission finds that
2	the program (or change) complies with the require-
3	ments of subsection (c).
4	(2) Form of application.—The Commission
5	shall accept an application for approval under para-
6	graph (1) in any reasonable form the applicant may
7	submit.
8	(3) Duration until renewal.—A self-regu-
9	latory program approved by the Commission under
10	paragraph (1) shall be approved for a period of 8
11	years.
12	(4) REVOCATION OF APPROVAL.—The Commis-
13	sion may, after notice and opportunity for a hearing,
14	revoke approval granted under paragraph (1), if the
15	Commission finds that a self-regulatory program
16	fails to meet the requirements of subsection (c).
17	(c) Requirements of Self-Regulatory Pro-
18	GRAM.—A self-regulatory program complies with the re-
19	quirements of this subsection if the program provides each
20	of the following:
21	(1) Guidelines and procedures requiring a pro-
22	gram participant to provide equivalent or greater
23	protections for consumers and their personally iden-
24	tifiable information as are provided under sections



	14
1	(2) Procedures and requirements to provide
2	for—
3	(A) an initial self-review and self-certifi-
4	cation of a participant's privacy policy and
5	practices to ensure compliance with the guide-
6	lines, procedures, requirements, and restrictions
7	of the program established under this sub-
8	section;
9	(B) subsequent periodic self-reviews and
10	self-certifications, which shall occur at least an-
11	nually, of the participant's privacy policy and
12	practices to ensure continued compliance with
13	such guidelines, procedures, requirements, and
14	restrictions;
15	(C) submission of self-reviews and self-cer-
16	tifications under this paragraph to any adminis-
17	trator of the program;
18	(D) random compliance testing of partici-
19	pants, and compliance testing of participants
20	with a high number of complaints against them,
21	to determine the tested participant's compliance
22	with the program; and
23	(E) regular compliance testing of a partici-
24	pant, which shall take place not less frequently

than every 4 years, with respect to the privacy



	10
1	policy and practices of the participant, to en-
2	sure that the self-reviews and self-certifications
3	of the participant are accurate and comply with
4	the program.
5	(3) Procedures and requirements that ensure
6	that a program participant provides a process for re-
7	solving disputes with consumers relating to the pri-
8	vacy policy and practices of the participant. Such
9	dispute resolution process—
10	(A) must be available without charge to a
11	consumer;
12	(B) must be available at a cost to the par-
13	ticipant that is reasonable and does not discour-
14	age participation by the participant in such
15	process;
16	(C) must ensure that consumers are in-
17	formed of how to utilize the process;
18	(D) may include, as one choice among oth-
19	ers, binding arbitration; and
20	(E)(i) must be completed within 30 days
21	after submission of the dispute by the con-
22	sumer; or
23	(ii) must be completed within 60 days after
24	submission of the dispute by the consumer, if

the participant—



	10
1	(I) determines that additional time is
2	required to obtain information to make an
3	informed decision with respect to the dis-
4	pute; and
5	(II) notifies the consumer that such
6	additional time is required.
7	(4) Provisions for the use by participants in the
8	program of a means (including the use of a seal) to
9	represent the participant's participation in the pro-
10	gram.
11	(5) With respect to any nonvoluntary suspen-
12	sion or termination of participation in the program
13	because of the participant's failure to comply with
14	the program, procedures or requirements to provide
15	for the following:
16	(A) Publication of notice and the reasons
17	for any such suspension or termination, except
18	that no personally identifiable information re-
19	lated to such suspension or termination may be
20	published.
21	(B) Notice to the Commission of any such
22	termination.
23	(6) Requirements and restrictions that assure
24	independence with respect to program eligibility,

compliance, and dispute resolution mechanisms and



	17
1	decisions from improper interference by management
2	or ownership of the self-regulatory program partici-
3	pant.
4	(7) A process for a noncompliant participant to
5	take timely remedial action in order to come back
6	into compliance with the program before suspension
7	or termination of participation in the program.
8	(d) Consumer Dispute Resolution.—
9	(1) Self-regulatory dispute process.—If
10	a consumer has a dispute with a participant in a
11	self-regulatory program under this section, the con-
12	sumer shall initially seek resolution through the par-
13	ticipant's dispute resolution process (established in
14	accordance with subsection (c)(3)). The Commission
15	shall promptly refer to the participant involved any
16	dispute submitted to the Commission for which reso-
17	lution has not been initially sought through such
18	process.
19	(2) Resolution by commission.—A consumer
20	may submit to the Commission for resolution a dis-
21	pute with a participant in a self-regulatory program

under this section, if the following requirements are



22

23

met:

1	(A) The dispute was initially submitted
2	under paragraph (1) for resolution through the
3	participant's dispute resolution process.
4	(B) The dispute submitted under para-
5	graph (1) is not resolved—
6	(i) within 30 days after submission of
7	the dispute by the consumer; or
8	(ii) to the satisfaction of the con-
9	sumer.
10	(C) Notice of the facts of the dispute is
11	submitted to the Commission not later than 30
12	days after the date on which the consumer is
13	notified of the resolution through the partici-
14	pant's dispute resolution process.
15	(D) The consumer has not voluntarily ac-
16	cepted a resolution of the dispute under para-
17	graph (1).
18	(E) The dispute was not resolved through
19	binding arbitration.
20	(e) Nonrelease of Certain Information.—The
21	Commission may not compel a participant in a self-regu-
22	latory program approved under subsection (b) (or an ad-
23	ministrator of such a program) to provide proprietary in-
24	formation or personally identifiable information of con-
25	sumers to the Commission unless the Commission provides



- 1 assurances that such information will not be released to
- 2 the public.
- 3 (f) Misrepresentation of Self-Regulatory
- 4 Program Participation.—It is unlawful for a data col-
- 5 lection organization to misrepresent that it is a participant
- 6 in a self-regulatory program (including through any mech-
- 7 anism provided under subsection (c)(4)) when such orga-
- 8 nization is not, in fact, such a participant.
- 9 (g) Exempted Entity Participation.—An entity
- 10 that is not a data collection organization and that volun-
- 11 tarily participates in a self-regulatory program under this
- 12 section shall enjoy the rights and benefits provided under
- 13 this section.
- 14 SEC. 107. ENFORCEMENT.
- 15 (a) Unfair or Deceptive Act or Practice.—A
- 16 violation of any provision of this title is an unfair or decep-
- 17 tive act or practice unlawful under section 5(a)(1) of the
- 18 Federal Trade Commission Act (15 U.S.C. 45(a)(1)), ex-
- 19 cept that the amount of any civil penalty under such Act
- 20 shall be doubled for a violation of this title, but may not
- 21 exceed \$500,000 for all related violations by a single viola-
- 22 tor (without respect to the number of consumers affected
- 23 or the duration of the related violations).
- 24 (b) Guidelines and Opinions.—In order to assist
- 25 in compliance with this title, the Federal Trade Commis-



- 1 sion may issue generally applicable guidelines and, upon
- 2 request, advisory opinions with respect specific types of
- 3 acts or practices that would, or would not, comply with
- 4 this title, but may not prescribe regulations to carry out
- 5 this title.

6 SEC. 108. NO PRIVATE RIGHT OF ACTION.

- 7 This title may not be considered or construed to pro-
- 8 vide any private right of action. No private civil action
- 9 relating to any act or practice governed under this title
- 10 may be commenced or maintained in any State court or
- 11 under State law (including a pendent State claim to an
- 12 action under Federal law).

13 SEC. 109. EFFECT ON OTHER LAWS.

- (a) QUALIFIED EXEMPTION FOR COMPLIANCE WITH
- 15 OTHER FEDERAL PRIVACY LAWS.—To the extent that
- 16 personally identifiable information protected under this
- 17 title is also protected under a provision of Federal privacy
- 18 law described in subsection (c), a data collection organiza-
- 19 tion that complies with the relevant provision of such other
- 20 Federal privacy law shall be deemed to have complied with
- 21 the corresponding provision of this title.
- 22 (b) Protection of Other Federal Privacy
- 23 Laws.—Nothing in this title may be construed to modify,
- 24 limit, or supersede the operation of the Federal privacy
- 25 laws described in subsection (c) or the provision of infor-



1	mation permitted or required, expressly or by implication,
2	by such laws, with respect to Federal rights and practices.
3	(c) Other Federal Privacy Laws Described.—
4	The provisions of law to which subsections (a) and (b)
5	apply are the following:
6	(1) Section 552a of title 5, United States Code
7	(commonly known as the Privacy Act of 1974).
8	(2) The Right to Financial Privacy Act of 1978
9	(12 U.S.C. 3401 et seq.).
10	(3) The Fair Credit Reporting Act (15 U.S.C.
11	1681 et seq.).
12	(4) The Fair Debt Collection Practices Act (15
13	U.S.C. 1692 et seq.).
14	(5) The Children's Online Privacy Protection
15	Act of 1998 (15 U.S.C. 6501 et seq.).
16	(6) Title V of the Gramm-Leach-Bliley Act of
17	1999 (15 U.S.C. 6801 et seq.).
18	(7) The Electronic Communications Privacy Act
19	of 1986 (Public Law 99–508).
20	(8) The Driver's Privacy Protection Act of
21	1994 (18 U.S.C. 2721 et seq.).
22	(9) The Family Educational Rights and Privacy
23	Act of 1974 (20 U.S.C. 1221 note, 1232g).
24	(10) Section 445 of the General Education Pro-

visions Act (20 U.S.C. 1232h).



1	(11) The Privacy Protection Act of 1980 (42
2	U.S.C. 2000aa et seq.).
3	(12) Section 222 of the Communications Act of
4	1934 (47 U.S.C. 222) relating to the Customer Pro-
5	prietary Network Information.
6	(13) The Cable Communications Policy Act of
7	1984 (47 U.S.C. 521 et seq.).
8	(14) The Communications Assistance for Law
9	Enforcement Act (47 U.S.C. 1001 et seq.).
10	(15) The Video Privacy Protection Act of 1988
11	(Public Law 100–618).
12	(16) The Telephone Consumer Protection Act
13	of 1991 (Public Law 102–243).
14	(17) The Health Insurance Portability and Ac-
15	countability Act of 1996 (Public Law 104–191), as
16	it relates to an entity described in section 1172(a)
17	of the Social Security Act (42 U.S.C. 1320d–1(a))
18	or to activities regulated under section 1173 of such
19	Act (42 U.S.C. 1320d–2).
20	(d) Preemption of State Privacy Laws.—This
21	title preempts any statutory law, common law, rule, or
22	regulation of a State, or a political subdivision of a State,
23	to the extent such law, rule, or regulation relates to or
24	affects the collection, use, sale, disclosure, or dissemina-

25 tion of personally identifiable information in commerce.



1	No State, or political subdivision of a State, may take any
2	action to enforce this title.
3	SEC. 110. EFFECTIVE DATE.
4	This title shall apply with respect to personally identi-
5	fiable information collected on or after the date that is
6	1 year after the date of enactment of this Act.
7	TITLE II—IDENTITY THEFT
8	PREVENTION AND REMEDIES
9	SEC. 201. FACILITATING ELECTRONIC IDENTITY THEFT AF-
10	FIDAVITS.
11	The Commission shall take such action as necessary
12	to permit (including by electronic means) consumers that
13	have a reasonable belief that they are a victim of identity
14	theft—
15	(1) to enter required consumer information in
16	the commission-developed document entitled "Iden-
17	tity Theft Affidavit"; and
18	(2) to submit completed forms and other sup-
19	plemental information to the Commission and other
20	entities.
21	SEC. 202. PROMOTING USE OF COMMON IDENTITY THEFT
22	AFFIDAVIT.
23	The Commission shall take such action as necessary
24	to solicit the acceptance and acknowledgement of stand-
25	ardized Identity Theft Affidavit by entities that receive



- 1 disputes regarding the unauthorized use of accounts of
- 2 such entities from consumers that have reason to believe
- 3 that they are a victim of identity theft.
- 4 SEC. 203. TIMELY RESOLUTION OF IDENTITY THEFT DIS-
- 5 PUTES.
- 6 The Commission shall require entities that receive
- 7 disputes regarding the unauthorized use of accounts of
- 8 such entities from consumers that have reason to believe
- 9 that they are a victim of identity theft to conduct any nec-
- 10 essary investigation and decide an outcome of a claim
- 11 within 90 days from the date on which all necessary infor-
- 12 mation to investigate the claim has been submitted to the
- 13 entity.
- 14 SEC. 204. IMPROVEMENTS TO CONSUMER CLEARING-
- 15 HOUSE.
- 16 The Commission shall utilize the Identity Theft
- 17 Clearinghouse to permit consumers that have a reasonable
- 18 belief that they are victim of identity theft to submit any
- 19 information relevant to such identity theft to the Clearing-
- 20 house (including by means of an Identity Theft Affidavit),
- 21 so that such information may be transmitted by the Clear-
- 22 inghouse to appropriate entities for necessary protective
- 23 action and to mitigate losses resulting from such identity
- 24 theft.



SEC. 205. IMPROVED IDENTITY THEFT DATA.

2 (a) In General.—The Cor	mmissi	ion shall—	
---------------------------	--------	------------	--

- 3 (1) establish a process to contact, not less than 4 annually, public and private entities that receive and 5 process complaints from consumers that have a rea-
- 6 sonable belief that they are a victim of identity theft;
- 7 and
- 8 (2) obtain accurate data on the incidences and 9 nature of complaints from such entitles.
- 10 (b) Inclusion in Database.—Such information
- 11 shall be made part of the Commission's Identity Theft
- 12 Clearinghouse database.

13 SEC. 206. CHANGE OF ADDRESS PROTECTIONS.

- 14 The Commission shall require appropriate entities to
- 15 take reasonable steps to verify the accuracy of a con-
- 16 sumer's address, including by confirming a consumer's
- 17 change of address by sending a confirmation of such
- 18 change to the old and the new address of the consumer.
- 19 SEC. 207. EFFECTIVE DATE.
- This title shall take effect 180 days after the date
- 21 of enactment of this Act.

22 TITLE III—INTERNATIONAL

PROVISIONS

- 24 SEC. 301. STUDY BY COMPTROLLER GENERAL.
- The Comptroller General of the United States shall
- 26 conduct a study and issue a report analyzing the impact



- 1 on the interstate and foreign commerce of the United
- 2 States of information privacy laws, regulations, or agree-
- 3 ments enacted, promulgated, or adopted by other nations,
- 4 including regional or international agreements between
- 5 nations, and whether the enforcement mechanisms or pro-
- 6 cedures of those laws, regulations, or agreements result
- 7 in discriminatory treatment of United States entities. The
- 8 first report under this section shall be issued not later
- 9 than 120 days after the date of enactment of this Act and
- 10 subsequent reports shall be issued every 3 years there-
- 11 after.
- 12 SEC. 302. REMEDIATION OF DISCRIMINATORY IMPACT BY
- 13 SECRETARY OF COMMERCE.
- 14 If the Comptroller General of the United States finds,
- 15 in the study and report under subsection (a), that such
- 16 information privacy laws, regulations, or agreements sub-
- 17 stantially impede interstate and foreign commerce of the
- 18 United States and that the enforcement mechanisms or
- 19 procedures of the information privacy laws, regulations,
- 20 or agreements described in such subsection result in dis-
- 21 criminatory treatment of United States entities, the Sec-
- 22 retary of Commerce shall, to the extent permitted by law
- 23 take all steps necessary to mitigate against such discrimi-
- 24 natory impact within 180 days after the report making
- 25 such findings is issued.



1 SEC. 303. EFFECT OF NONREMEDIATION.

- 2 (a) RECOMMENDATIONS.—If by the end of the 180-
- 3 day period described in section 302, the Secretary of Com-
- 4 merce has not attained complete relief from the discrimi-
- 5 natory impact described in such subsection, the Secretary
- 6 shall report to the Congress and the President rec-
- 7 ommendations on action to relieve any such remaining dis-
- 8 criminatory impact.
- 9 (b) Federal Agency Action After Consider-
- 10 ATION BY CONGRESS.—During the period after the Sec-
- 11 retary reports recommendations under subsection (b) for
- 12 mitigation of discriminatory impact and before the Con-
- 13 gress acts with respect to such recommendations, no offi-
- 14 cer or employee of any Federal agency may take or con-
- 15 tinue any action to enjoin, or impose any penalty on, a
- 16 United States entity, or a citizen or legal resident of the
- 17 United States, for the purpose of fulfilling an international
- 18 obligation of the United States under an international pri-
- 19 vacy agreement (other than such an obligation under a
- 20 ratified treaty) that resulted in such discriminatory im-
- 21 pact.
- 22 SEC. 304. HARMONIZATION OF INTERNATIONAL PRIVACY
- 23 LAWS, REGULATIONS, AND AGREEMENTS.
- 24 Beginning on the date of enactment of this Act, the
- 25 Secretary of Commerce shall provide notice of the provi-
- 26 sions of this Act to other nations, individually, or as mem-



1	bers of international organizations or unions that have en-
2	acted, promulgated, or adopted information privacy laws,
3	regulations, or agreements, and shall seek recognition of
4	this Act by such nations, organizations, or unions. The
5	Secretary shall seek the harmonization of this Act with
6	such information privacy laws, regulations, or agreements,
7	to the extent such harmonization is necessary for the ad-
8	vancement of transnational commerce, including electronic
9	commerce.
10	TITLE IV—GENERAL
11	PROVISIONS
12	SEC. 401. DEFINITIONS.
13	In this Act:
14	(1) The term "Commission" means the Federal
15	Trade Commission.
16	(2) The term "consumer" means an individual
17	acting in the individual's personal, family, or house-
18	hold capacity.
19	(3)(A) The term "data collection organization"
20	means an entity (or an agent or affiliate of the enti-
21	ty) that collects (by any means, through any me-
22	dium), sells, discloses for consideration, or uses per-
23	sonally identifiable information of the consumer.
24	

(i) a governmental agency; or



1	(ii) a not-for-profit entity, to the extent
2	that personally identifiable information is not
3	used for a commercial purpose; or
4	(iii) an entity that—
5	(I) has annual gross revenue under
6	\$1,000,000 (based on the value of such
7	amount in fiscal year 2000, adjusted for
8	current dollars);
9	(II) has fewer than 25 employees;
10	(III) collects or uses personally identi-
11	fiable information from fewer than 1,000
12	consumers for a purpose unrelated to a
13	transaction with the consumer;
14	(IV) does not process personally iden-
15	tifiable information of consumers; and
16	(V) does not sell or disclose for con-
17	sideration such information to another per-
18	son.
19	(4)(A) The term "personally identifiable infor-
20	mation", with respect to a data collection organiza-
21	tion means individually identifiable information re-
22	lating to a living individual who can be identified
23	from that information.
24	(B) Such term includes—



	9 0
1	(i) first and last name, whether given at
2	birth or adoption, assumed, or legally changed
3	(ii) home or other physical address includ-
4	ing street name and name of a city or town;
5	(iii) electronic mail address;
6	(iv) telephone number;
7	(v) social security number; or
8	(vi) any other unique identifying informa-
9	tion that a data collector and processor collects
10	and combines with any information described in
11	the preceding subparagraphs of this paragraph
12	(C) Such term does not include—
13	(i) anonymous or aggregate data, or
14	any other information that does not iden-
15	tify a unique living individual;
16	(ii) information about a consumer in-
17	ferred from data maintained about a con-
18	sumer; or
19	(iii) information about a consumer ob-
20	tained from a public record.
21	(5) The term "affiliate" means any company
22	that controls, is controlled by, or is under common
23	control with another company.
24	(6) The term "information-sharing partner"

means, with respect to a data collection organiza-



1	tion, an entity that is contractually obligated to com-
2	ply with the practices enumerated under the privacy
3	policy statement of the organization required under
4	section 102.
5	(7) The term "process", with respect to person-
6	ally identifiable information, means any value-added
7	activity performed on data by automated means.
8	(8) The term "transaction" means an inter-
9	action between a consumer and a data collection or-
10	ganization resulting in—
11	(A) any use of information that is nec-
12	essary to complete the interaction in the course
13	of which information is collected, or to maintain
14	the provisioning of a good or service requested
15	by the consumer, including use—
16	(i) to approve, guarantee, process, ad-
17	minister, complete, enforce, provide, or
18	market a product, service, account, benefit,
19	transaction, or payment method that is re-
20	quested or approved by the consumer; or
21	(ii) to deliver goods, services, funds,
22	or other consideration to, or on behalf of,

the consumer;



	02
1	(B) any disclosure of information that is
2	necessary for the consumer to enforce any right
3	of the consumer;
4	(C) any disclosure of information that is
5	required by law or by a court order; and
6	(D) any use of information to evaluate, de-
7	tect, or reduce the risk of fraud or other crimi-
8	nal activity, or other risk-management activi-
9	ties.
10	(9) The term "display" means intentionally
11	communicating or otherwise making available (on
12	the Internet or in any other manner) to another per-
13	son.
14	(10) The term "public record" means any item,
15	collection, or grouping of information about an indi-
16	vidual that is maintained by a Federal, State, or
17	local government entity and that is made available
18	to the public.
19	(11) The term "purchase" means providing, di-
20	rectly or indirectly, anything of value in exchange
21	for a benefit.
22	(12) The term "State" includes the several
23	States, the District of Columbia, the Commonwealth
24	of Puerto Rico, the Commonwealth of the Northern

Mariana Islands, American Samoa, Guam, the Vir-



- 1 gin Islands, the Freely Associated States, and any
- 2 other territory or possession of the United States.

